UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/353,270	07/14/1999	SUSUMU KUSAKABE	450100-4984	3256

20999 7590 01/31/2005

FROMMER LAWRENCE & HAUG
745 FIFTH AVENUE- 10TH FL.
NEW YORK, NY 10151

EXAMINER	
GYORFI, THOMAS A	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 01/31/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/353,270	KUSAKABE ET AL.	
	Examiner	Art Unit	
	Tom Gyorfi	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 August 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *39-42,44-49,51,52 and 54* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *39-42,44-49,51,52 and 54* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 39-42, 44-49, 51-52, and 54 are pending. The correspondence filed 8/3/04 amended claims 39, 44, 51, 52, and 54.

Response to Arguments

2. Applicant's arguments filed 8/3/04 have been fully considered but they are not persuasive. Applicant argues, "*Daughters discloses a check byte that 'is used to detect distorted data in a data record' (column 9, lines 41-49). Therefore, the check byte of the IC card 'checks the integrity of the data' in order to determine and record whether or not there are any defective locations within the data. In contrast, the check code of the present invention is used to prevent un-authorized users from accessing certain data stored in the information processing device. Furthermore, the check code of the present invention is encrypted with the management information. Daughters does not encrypt the check byte. Tuttle relates to protecting data on smart cards (column 1, lines 5-8). However, Tuttle does not teach or suggest a check code to check whether management information has been tampered with by a non-authorized user, nor an encrypting means for encrypting the check code. Specifically, Tuttle does not mention anything concerning check codes and is not concerned with check codes because Tuttle utilizes passwords (as opposed to check codes) to deny access to certain users (column 6, lines 5-21). Therefore, the instant claims are believed to be distinguishable from the applied combination of Daughters and Tuttle for at least the reasons stated above.*" Examiner disagrees with this contention. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). In this case, Tuttle clearly teaches that data on a smart card can be

encrypted, using a password or PIN number (Tuttle, col. 2, line 64 – col. 3, line 6). It would have been obvious to one of ordinary skill in the art at the time the invention was made to encrypt the data stored on the card disclosed by Daughters, including the check code, using the various means taught by Tuttle. The motivation for doing so would be to make the data on the card more tamper-resistant and defending it from being accessed by unauthorized individuals (Tuttle, col. 3, lines 17-27). It should also be noted that the check byte as disclosed by Daughters "is used to detect distorted data in a data record." (Daughters, col. 9, line 41-42). The check byte is clearly seen to function as a checksum, which is a feature that is well known in the art as a means to detect any alteration of data, regardless of cause. As such, the check byte disclosed in Daughters is thus construed to function in the manner disclosed in the claims of the instant application.

Claim Rejections - 35 USC § 103

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

4. Claims 39-42, 44-49, 51-52, and 54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Daughters et al. (U.S. Patent 4,742,215) and further in view of Tuttle et al. (U.S. Patent 5,988,510)

Referring to Claims 39 and 52:

Daughters discloses an information processing device for supplying management information to a data storage device, said information processing device comprising:

forming means for forming management information that manages a storage area in the data storage device in a layered structure, said management information pertaining to a definition area to be formed in the data storage device, said definition area being used to define storage areas of the data storage device for use in providing services (col 3, lines 20-30);

communication means for communicating the encrypted management information to said data storage device, to enable said definition area to be formed therein based upon said management information (col 3, lines 10-55); and

means for generating a check code to check whether the management information has been tampered with by a non-authorized user, wherein said encrypting means encrypts the check code together with the management information (col 9, lines 25-45).

Daughters does not explicitly discloses "encrypting means for encrypting said management information, said encrypting means encrypting a lower layer of the management information by using a key contained in an upper layer of the management information".

Tuttle discloses encrypting means for encrypting said management information, said encrypting means encrypting a lower layer of the management information by using a key contained in an upper layer of the management information (col 6, lines 35-60).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the teachings of Daughter such that the management information is encrypted. One of ordinary skill in the art would have been motivated to do this because it would prevent unauthorized reading of the storage and private information (col 6, lines 5-20).

Referring to Claim 40:

Daughters in view of Tuttle disclose the limitations of Claim 39 above. Tuttle further discloses said communication means is configured to transmit the encrypted management information through a predetermined transmission medium (col 6, lines 30-40).

Referring to Claim 41:

Daughters in view of Tuttle disclose the limitations of Claim 39 above. Daughters further discloses said forming means forms said management information such that the management information contains a storage area identifying code to be allocated to a storage area of the data storage device to be managed, and is used to identify said storage area (col 9, lines 55-65 and col 10, lines 25-55).

Referring to Claim 42:

Daughters in view of Tuttle disclose the limitations of Claim 39 above. Daughters further discloses said forming means forms said management information such that said management information contains information on the amount of empty capacity of said storage area to be managed (col 13, line 55-col 14, line 5).

Referring to Claims 44 and 54:

Daughters disclose a data storage device comprising: receiving means for receiving encrypted management information from an external equipment, said management information pertaining to a definition area to be formed in the data storage device, said definition area being used to define storage areas of the data storage device for use in providing services, wherein said storage areas are managed with management information in a layer structure and containing a key (col 9, line 55-col 10, line 15);

management information storage means for storing the management information; and management means for forming the definition area defining said storage areas in a layered structure, and also managing the storage areas, on the basis of the received management information (col 10, lines 1-22), and

operation means for operating on a cheek code to check whether the management information has been tampered with by a non-authorized user, wherein said decrypting means decrypts the check code together with the management information (col 9, lines 40-50).

Tuttle discloses decrypting means for decrypting a lower layer of the encrypted management information by using said key, said key being contained in an upper layer of the management information; data storage means for storing data to supply predetermined services, wherein access to a storage area of said data storage means is provided by said key (col 6, lines 10-20);

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the teachings of Daughter such that the management information is decrypted. One of ordinary skill in the art would have been motivated to do this because it would prevent unauthorized reading of the storage and private information (col 6, lines 5-20).

Referring to Claim 45:

Daughters in view of Tuttle disclose the limitations of Claim 44 above. Tuttle further discloses said receiving means provides access to said external equipment through a predetermined transmission medium (col 6, lines 30-40).

Referring to Claim 46:

Daughters in view of Tuttle disclose the limitations of Claim 44 above. Daughters further discloses said management means is arranged to manage said storage areas in response to an instruction from said external equipment (col 3, lines 15-55).

Referring to Claim 47:

Daughters in view of Tuttle disclose the limitations of Claim 44 above. Tuttle further discloses said receiving means is arranged to perform the communications with said external equipment in a contact or non-contact state (col 5, lines 40-65; col 6, line 65-col 7, line 10).

Referring to Claim 48:

Daughters in view of Tuttle disclose the limitations of Claim 44 above. Daughters further discloses said management information contains a storage area identifying code which can be allocated to said storage area to be managed and is used to identity said storage area (col 14, lines 25-60).

Referring to Claim 49:

Daughters in view of Tuttle disclose the limitations of Claim 44 above. Daughters further disclose said management information contains information on the amount of an empty capacity of said storage area to be managed (col 13, line 65-col 14, line 5).

Referring to Claim 51:

Daughters discloses an information processing system comprising a data storage device and an information processing device, said information processing device comprising: forming means for forming management information that manages a storage area in the data storage device in a layered structure (col 3, lines 20-60);

and communication means for communicating the encrypted management information to said data storage device, said data storage device comprising: receiving means for receiving encrypted management information from said information processing device (col 8, lines 20-35; col 10, lines 25-55);

data storage means for storing data to supply a predetermined service, wherein access to a storage area of said data storage means is provided by said key; management information storage means for storing said management information (col 10, lines 15-25); and

management means for forming a definition area defining the storage areas of said data storage means in a layer structure, and also managing the storage areas, on the basis of the received management information (col 10, lines 1-25); and means for generating a check code to check whether the management information has been tampered with by a non-authorized user, wherein said encrypting means encrypts the check code together with the management information (col 9, lines 40-50).

Daughter does not explicitly disclose "encrypting means for encrypting said management information, said encrypting means encrypting a lower layer of the management information by using a key contained in an upper layer of the management information; and

decrypting means for decrypting the lower layer of the encrypted management information by using the key contained in the upper layer of the management information".

Tuttle discloses encrypting means for encrypting said management information, said encrypting means encrypting a lower layer of the management information by using a key contained in an upper layer of the management information (col 6, lines 10-20); and

decrypting means for decrypting the lower layer of the encrypted management information by using the key contained in the upper layer of the management information (col 6, lines 30-45).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the teachings of Daughters such that information is encrypted. One of ordinary skill in the art would have been motivated to do this because it would prevent unauthorized access to the data stored in the ROM (col 6, lines 40-68).

Conclusion

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tom Gyorfi whose telephone number is (571) 272-3849. The examiner can normally be reached on 8:00am - 4:30pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

TAG
1/26/05

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 21